

PA 334163

REC'D 12 DEC 2000

WIPRO DOT

PO PCT

1/00/591

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME;

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

November 27, 2000

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM
THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK
OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT
APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A
FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: 60/155,568

FILING DATE: *September 24, 1999*

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

**By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS**



H. L. Jackson
H. L. JACKSON
Certifying Officer

66/42/60
15535 U.S. PTO

PROVISIONAL APPLICATION COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION under 37 CFR § 1.53 (b)(2).

		Docket Number	1684/3	Type a plus sign (+) inside this box-->	+
INVENTOR(s)/APPLICANT(s)					
LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)		
ZAROM	RONY		KFAIR SABA, ISRAEL		
MIZRACHI	YAROH		KFAIR SABA, ISRAEL		
TITLE OF THE INVENTION (280 characters max)					
SYSTEM AND METHOD FOR PROCESSING RULES FOR FILTERING PACKETS ON A NETWORK					
CORRESPONDENCE ADDRESS					
Mark M. Friedman, c/o CASTORINA, 2001 Jefferson Davis Highway, Suite 207, Arlington					
STATE	Virginia	ZIP CODE	22202	COUNTRY	USA
ENCLOSED APPLICATION PARTS (check all that apply)					
<input checked="" type="checkbox"/> Specification	Number of Pages	15	<input type="checkbox"/> Small Entity Statement		
<input checked="" type="checkbox"/> Drawing(s)	Number of Sheets	3	<input type="checkbox"/> Other (specify)		
METHOD OF PAYMENT (check one)					
<input type="checkbox"/>	A check or money order is enclosed to cover the Provisional filing fees			PROVISIONAL FILING FEE AMOUNT(\$)	\$150.00
<input checked="" type="checkbox"/>	The Commissioner is hereby authorized to charge filing fees and credit Deposit Account Number:			06-2140	

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

 No Yes, the name of the U.S. Government agency and the Government contract number are: _____

CERTIFICATE OF EXPRESS MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Invoice No.:
in an envelope addressed to:

Commissioner of Patents and Trademarks
Box Provisional Patent Application
Washington, D.C. 20231

on this _____ day of _____ 1996.

Respectfully submitted,

SIGNATURE

TYPED or PRINTED NAME MARK M. FRIEDMANDate 21 SEP 95
REGISTRATION NO. 33,883 Additional inventors are being named on separately numbered sheets attached hereto

PROVISIONAL APPLICATION FILING ONLY

PROVISIONAL APPLICATION

Inventors: Rony Zarom and Yarom Mizrachi

Title: SYSTEM AND METHOD FOR PRESORTING RULES FOR
FILTERING PACKETS ON A NETWORK

5

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a system and method for presorting rules for filtering packets on a network, and in particular for presorting such rules according a user profile.

10 Security of information is extremely important for modern society, particularly since the advent of the Internet. Unauthorized exposure of such information, and/or unintended or unauthorized use of information may significantly damage organizations and individuals. Damage may also be caused by lost, corrupted or misused information. Thus, appropriate security
15 measures are required in order to protect information from such damaging actions, while still maintaining the availability of such information to authorized individuals and/or organizations.

Currently, flexibility and ease of access to information are highly valued, particularly through the Internet and organizational intranets, which provide
20 connections between computers through a network. Accessing information through a network enables users at physically separate locations to share information, but also increases the possibility of unauthorized or unintended access to the information. Various attempts to provide a solution to the

problem of security for electronically stored information are known in the art, but all of these attempted solutions have various drawbacks.

For example, a "firewall" is a software program or hardware device which attempts to provide security to an entire network, or to a portion thereof,

5 by filtering all communication which passes through an entry point to the entire network or the portion of the network. The filtration of packets is performed according to one or more rules, such that if the packet does not conform to these rules, then the packet is blocked from entry to the entry point. An example of such a firewall is disclosed in U.S. Patent No. 5,606,668,

10 incorporated by reference as if fully set forth herein.

Unfortunately, currently available firewalls have a number of disadvantages. In particular, these firewalls can be extremely slow and non-selective in terms of the application of the rules. For example, U.S. Patent No. 5,606,668 neither teaches nor suggests a step of presorting the rules according

15 to a characteristic of the packet. Such presorting could significantly reduce the number of rules which would need to be examined in reference to the packet, and hence would greatly increase the speed of filtering packets. Unfortunately, a firewall with such presorting is not currently available.

There is thus a need for, and it would be useful to have, a system and a

20 method for presorting rules for application to a packet as part of a network security filter according to a characteristic of the packet, and preferably according to at least one of the source address and destination address, thereby

reducing the number of rules which must be applied to the packet in order to increase the rate of filtering.

BRIEF DESCRIPTION OF THE DRAWINGS

5 The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, wherein:

FIG. 1 is a schematic block diagram of a system according to the present invention; and

10 FIG. 2 is a flowchart of a method according to the present invention.

SUMMARY OF THE INVENTION

The present invention is of a method and a system for presorting rules for filtering a packet in a network security filter according to a characteristic of 15 the packet, preferably at least one of the source address and destination address.

The advantage of presorting rules before application to the packet is that the number of rules which must be examined should be significantly reduced. In addition, the source address and/or destination address can be associated with a particular profile, which may be associated with a particular user for example.

20 The rules are also more easily managed according to such profiles, since the network manager or system administrator can choose a set of rules for the profile, and then amend the profile as a whole, rather than attempting to apply disparate, unrelated rules for filtering. Thus, the method and system of the

present invention are more efficient both for actual filtering of packets, and for management of the security network filter.

According to the present invention, there is provided a method for presorting a plurality of rules for filtering a packet in network, the method 5 comprising the steps of: (a) selecting a characteristic for sorting the plurality of rules, the characteristic having a plurality of possible values; (b) associating each rule with at least one value for the characteristic; (c) receiving the packet; (d) at least partially analyzing information in the packet to obtain the value for 10 the characteristic; (e) selecting at least one of the plurality of rules according to the value to form at least one selected rule; and (f) applying the selected rule to the packet, such that the packet is permitted to enter the network or alternatively is dropped.

Hereinafter, the term "network" refers to a connection between any two electronic devices which permits the transmission of data.

15 Hereinafter, the term "security network filter" also refers to firewalls and any other type of mechanism for filtering packets according to one or more rules.

Hereinafter, the term "wireless device" refers to any type of electronic device which permits data transmission through a wireless channel, for example 20 through transmission of radio waves. Hereinafter, the term "cellular phone" is a wireless device designed for the transmission of voice data and/or other data, through a connection to the PSTN (public switched telephone network) system.

Hereinafter, the term "computer" includes, but is not limited to, personal

computers (PC) having an operating system such as DOS, Windows™, OS/2™ or Linux; Macintosh™ computers; computers having JAVA™-OS as the operating system; and graphical workstations such as the computers of Sun Microsystems™ and Silicon Graphics™, and other computers having some

5 version of the UNIX operating system such as AIX™ or SOLARIS™ of Sun

~~Microsystems™; or any other known and available operating system~~

Hereinafter, the term "Windows™" includes but is not limited to

Windows95™, Windows 3.x™ in which "x" is an integer such as "1", Windows

NT™, Windows98™, Windows CE™ and any upgraded versions of these

10 operating systems by Microsoft Corp. (USA).

The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware or firmware, or a combination thereof. For the present invention, a software application could be written in substantially any suitable programming language, which could easily be selected by one of ordinary skill in the art. The programming language chosen should be compatible with the computer hardware and operating system according to which the software application is executed. Examples of suitable programming languages include, but are not limited to, C, C++ and Java.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is of a method and a system for presorting rules for filtering a packet in a network security filter according to a characteristic of the packet. The characteristic is preferably at least one of the source address and destination address. The advantage of presorting rules before application to the packet is that the number of rules which must be examined should be

significantly reduced. Furthermore, those rules which are selected after the presorting procedure for application to the packet are therefore more relevant to that particular packet, such that the analysis of the packet is more efficient.

10 In addition, the source address and/or destination address can be associated with a particular profile, which may be associated with a particular user for example. The rules are also more easily managed according to such profiles, since the network manager or system administrator can choose a set of rules for the profile, and then amend the profile as a whole, rather than 15 attempting to apply disparate, unrelated rules for filtering. For example, different levels of user permissions may be determined according to company policy, such that a basic profile for each level of permission would be provided.

The system administrator or network manager would therefore select the profile, which would already contain all of the necessary general rules.

20 Optionally, if necessary, one or more changes to the rules could be made in order to fully optimize the rules for the particular source and/or destination address for that user. Thus, the method and system of the present invention are more efficient both for actual filtering of packets, and for management of the

security network filter.

The principles and operation of a system and a method according to the present invention may be better understood with reference to the drawings and the accompanying description, it being understood that these drawings are

5 given for illustrative purposes only and are not meant to be limiting.

Referring now to the drawings, Figure 1 is a schematic block diagram of an exemplary system 10 according to the present invention for filtering packets according to a plurality of presorted rules. System 10 features a network 12 with an entry point 14, which is preferably a computer connected to network

10 12. Preferably, all network traffic must pass through entry point 14 for transmission on network 12, although a plurality of such entry points 14 may optionally be present on network 12 (not shown). Network 12 also features a plurality of endpoint computers 16 for transmitting and receiving packets. Each such endpoint computer 16 features an address, such that each packet has a 15 source address, which may be from an endpoint computer 16 within network 12 or from a network entity outside network 12, and a destination address, which is within network 12. In the simplified network shown, the destination address would be for an endpoint computer 16. It is understood that the structure of network 12 has been simplified for the sake of clarity, and is not meant to be 20 limiting in any way. Furthermore, techniques for constructing various configurations of networks are well known to those of ordinary skill in the art. The present invention is operative with any possible network configuration.

A network security filter 18 is installed at entry point 14. As described previously, network security filter 18 may be implemented as software, hardware, firmware or a combination thereof. Network security filter 18 must have access to packets being transmitted through entry point 14. Network

5 security filter 18 then first retrieves at least one characteristic of the packet, which is preferably at least one of a source address and a destination address of

the packet, and uses this characteristic to presort a plurality of filtering rules which are stored in a rules database 20. Only those rules which are indicated as being relevant for that value of the characteristic, such as a particular source

10 address or destination address, or combination thereof, are then applied to the packet by network security filter 18. The process of applying the rules involves further analysis of the packet to obtain the necessary information, and then comparing the information in the packet to the rule, such that if the rule is not fulfilled, the packet is rejected or dropped. The dropped packet cannot then

15 enter network 12 through entry point 14. Optionally and additionally, an alarm or other indication is given, and/or an entry is made in a log file, if one or more rules are violated by the packet.

Preferably, the rules contained in rules database 20 are presorted according to a plurality of possible values for the characteristic which is

20 examined, more preferably with a default value. Therefore, when the characteristic of the packet is analyzed and the value is retrieved, network security filter 18 is able to quickly retrieve only those rules from rules database

20. Alternatively, the rules may not be presorted, but may instead be sorted separately for each incoming packet by network security filter 18.

As previously described, and as described in greater detail below with regard to Figure 2, the characteristic which is preferably retrieved from the 5 packet in order to sort the rules is at least one of the source address and the destination address of the packet. The source address and/or the destination address may be associated with a particular user, such that the permissions and restrictions placed upon the behavior of the user within network 12 are reflected in terms of the rules applied to packets associated with that user. Using the 10 source address and/or the destination address as the characteristic for sorting the rules has the advantage that users who are located at computers outside of network 12 (not shown) may be accorded certain privileges for entry through entry point 14. Thus, a user who is working at home, while traveling, or at a remote office, for example, may be granted certain privileges in terms of the 15 permitted behavior of the packet.

With regard to the actual application of the rules to the packets, as well as of the construction of the rules themselves, these aspects of filtering the packets are known in the background art. In particular, these functions are described in U.S. Patent No. 5,606,668, previously incorporated by reference.

20. Briefly, a packet enters entry point 14 and passes through layers 1 and 2 of the ISO (International Standardization Organization) model of communication protocol layers for a network. The packet is then diverted to network security filter 18. Network security filter 18 then analyzes information contained within

the packet, which may for example optionally include information in one of the headers or alternatively the data being carried by the packet. Preferably, the packet is analyzed from the uppermost header, which is the IP (Internet Protocol) header, to the data being carried, such that each layer of information

5 is retrieved from the packet and compared to one or more rules. If at least one rule is violated, then either network security filter 18 drops the packet, or at

least indicates the presence of a rules violation. If network security filter 18 determines that a terminal violation has occurred, such that the packet is forbidden to enter network 12 because of the particular violation, the analysis is

10 preferably stopped and the packet is dropped.

Figure 2 is a flowchart of an exemplary method for preparing a user profile, and for then applying the presorted rules to a received packet. In step 1, the characteristic for sorting the rules is selected. Preferably, the characteristic is at least one of the source address of the packet and the destination address of

15 the packet, and is more preferably a combination thereof. In step 2, a plurality of rules are constructed. For example, a rule may be simple, such that no incoming connections to a particular port associated with a particular service are permitted. Optionally, a rule may be complex, involving a variety of factors such as the source address of the packet, the type of application generating the

20 data contained in the packet and so forth. In step 3, optionally users who are associated with a value for the characteristic are given a particular level of permissions and privileges, which then constitute the user profile. For example,

users at a certain level may not have permission to receive HTML (HyperText Mark-up Language) documents, such that they cannot download Web pages.

In step 4, each rule is associated with at least one value for the selected characteristic, and preferably is associated with a plurality of such values. For 5 example, each rule may be associated with at least one source address, or a class of such source addresses which may be defined by grouping the users associated with those addresses into certain levels of permissions, as previously described. If a user profile is available, preferably the restrictions and privileges contained therein are used to associate each rule with one or more 10 values for the selected characteristic. In step 5, optionally and preferably, the rules are presorted according to the associated value or values for the selected characteristic, in order to facilitate later application of the rule to information contained in the packet.

In step 6, a packet is received by the network security filter. In step 7, 15 the information contained in the packet is at least partially analyzed in order to obtain the value for each characteristic which is used to sort the rules. As previously described, this characteristic is preferably at least one of the source address and destination address. In step 8, the value or values are used to selected the rule(s) which are to be applied. In step 9, the rules are applied, 20 such that the packet is either permitted to enter the network or is dropped.

It will be appreciated that the above descriptions are intended only to serve as examples, and that many other embodiments are possible within the

spirit and the scope of the present invention.

6015558.0246

WHAT IS CLAIMED IS:

1. A method for presorting a plurality of rules for filtering a packet in network, the method comprising the steps of:

- (a) selecting a characteristic for sorting the plurality of rules, said characteristic having a plurality of possible values;
- (b) associating each rule with at least one value for said characteristic;
- (c) receiving the packet;
- (d) at least partially analyzing information in the packet to obtain said value for said characteristic;
- (e) selecting at least one of the plurality of rules according to said value to form at least one selected rule; and
- (f) applying said selected rule to the packet, such that the packet is permitted to enter the network or alternatively is dropped.

2. The method of claim 1, wherein the plurality of rules are presorted according each value for said characteristic.

3. The method of claim 2, wherein said characteristic is at least one of a source address of the packet and a destination address of the packet.

4. The method of claim 3, wherein said characteristic is a combination of said source address of the packet and said destination address of the packet.

5. The method of claim 3, wherein a user is associated with each value of said characteristic, such that step (b) further comprises the steps of:

- (i) assigning at least one privilege to said user; and
- (ii) determining whether to associate each rule with said value of said characteristic according to said at least one privilege.

6. The method of claim 5, wherein step (i) further comprises the step of determining a user profile of associated rules according to said at least one privilege.

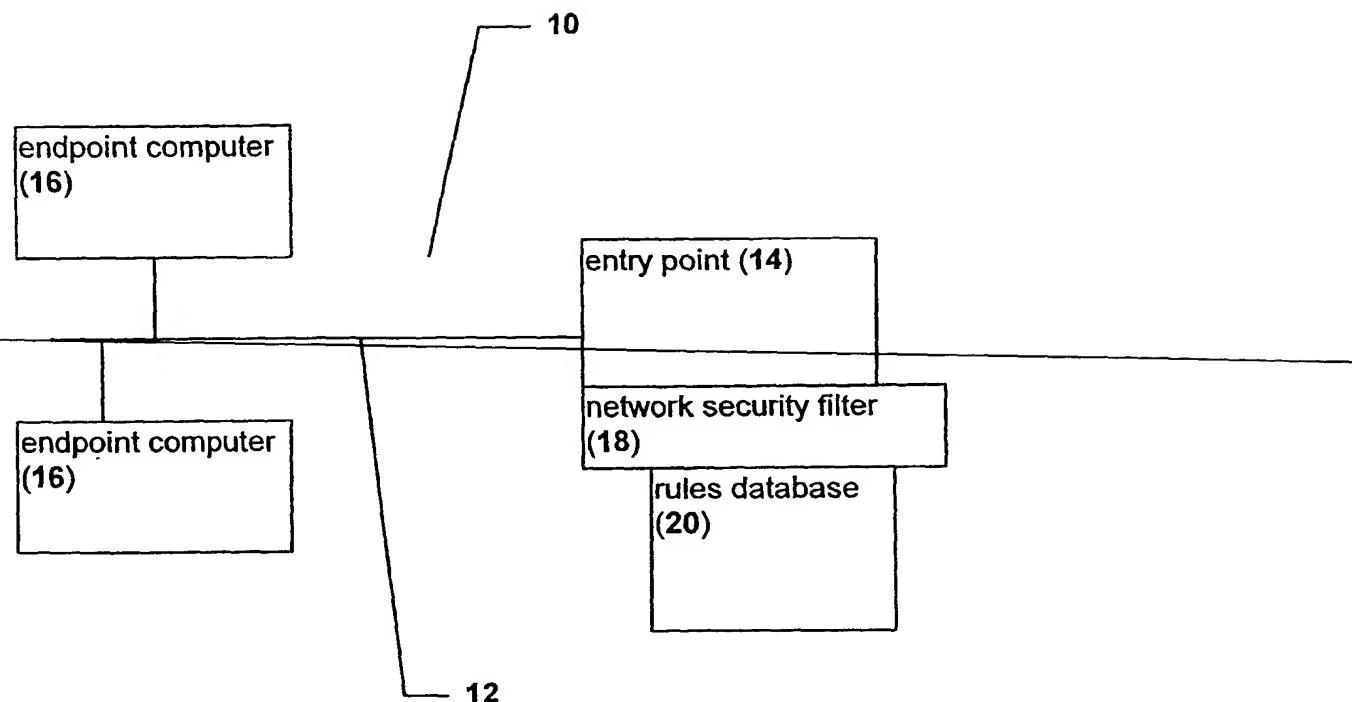
7. The method of claim 6, wherein said user profile is further associated with a group profile, such that a plurality of values for said characteristic is associated with said associated rules of said group profile.

ABSTRACT OF THE DISCLOSURE

A method and a system for presorting rules for filtering a packet in a network security filter according to a characteristic of the packet, preferably according to at least one of the source address and destination address. The advantage of presorting rules before application to the packet is that the number of rules which must be examined should be significantly reduced. In addition, the source address and/or destination address can be associated with a particular profile, which may be associated with a particular user for example. The rules are also more easily managed according to such profiles, since the network manager or system administrator can choose a set of rules for the profile, and then amend the profile as a whole, rather than attempting to apply disparate, unrelated rules for filtering. Thus, the method and system of the present invention are more efficient both for actual filtering of packets, and for management of the security network filter.

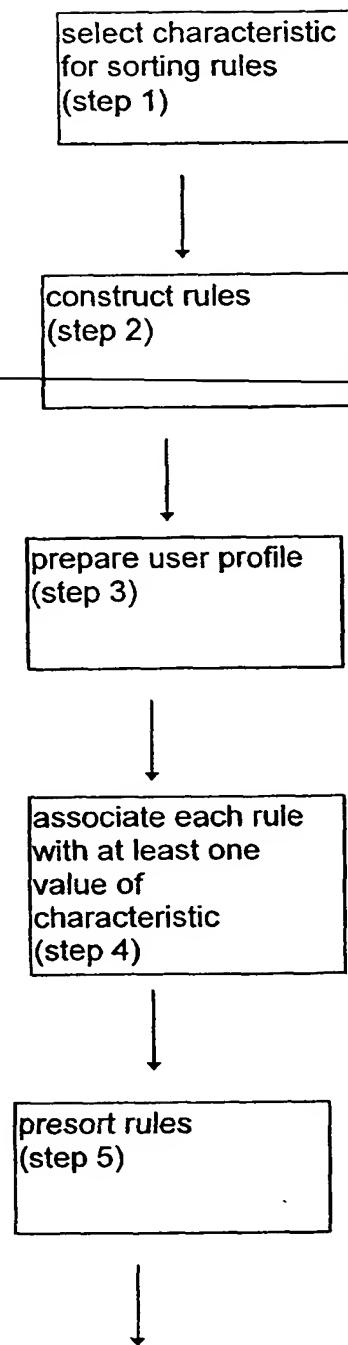
235956 6 2435

Figure 1



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
7010
7011
7012
7013
7014
7015
7016
7017
7018
7019
7020
7021
7022
7023
7024
7025
7026
7027
7028
7029
7030
7031
7032
7033
7034
7035
7036
7037
7038
7039
7030
7031
7032
7033
7034
7035
7036
7037
7038
7039
7040
7041
7042
7043
7044
7045
7046
7047
7048
7049
7040
7041
7042
7043
7044
7045
7046
7047
7048
7049
7050
7051
7052
7053
7054
7055
7056
7057
7058
7059
7050
7051
7052
7053
7054
7055
7056
7057
7058
7059
7060
7061
7062
7063
7064
7065
7066
7067
7068
7069
7060
7061
7062
7063
7064
7065
7066
7067
7068
7069
7070
7071
7072
7073
7074
7075
7076
7077
7078
7079
7070
7071
7072
7073
7074
7075
7076
7077
7078
7079
7080
7081
7082
7083
7084
7085
7086
7087
7088
7089
7080
7081
7082
7083
7084
7085
7086
7087
7088
7089
7090
7091
7092
7093
7094
7095
7096
7097
7098
7099
7090
7091
7092
7093
7094
7095
7096
7097
7098
7099
7100
7101
7102
7103
7104
7105
7106
7107
7108
7109
7100
7101
7102
7103
7104
7105
7106
7107
7108
7109
7110
7111
7112
7113
7114
7115
7116
7117
7118
7119
7110
7111
7112
7113
7114
7115
7116
7117
7118
7119
7120
7121
7122
7123
7124
7125
7126
7127
7128
7129
7120
7121
7122
7123
7124
7125
7126
7127
7128
7129
7130
7131
7132
7133
7134
7135
7136
7137
7138
7139
7130
7131
7132
7133
7134
7135
7136
7137
7138
7139
7140
7141
7142
7143
7144
7145
7146
7147
7148
7149
7140
7141
7142
7143
7144
7145
7146
7147
7148
7149
7150
7151
7152
7153
7154
7155
7156
7157
7158
7159
7150
7151
7152
7153
7154
7155
7156
7157
7158
7159
7160
7161
7162
7163
7164
7165
7166
7167
7168
7169
7160
7161
7162
7163
7164
7165
7166
7167
7168
7169
7170
7171
7172
7173
7174
7175
7176
7177
7178
7179
7170
7171
7172
7173
7174
7175
7176
7177
7178
7179
7180
7181
7182
7183
7184
7185
7186
7187
7188
7189
7180
7181
7182
7183
7184
7185
7186
7187
7188
7189
7190
7191
7192
7193
7194
7195
7196
7197
7198
7199
7190
7191
7192
7193
7194
7195
7196
7197
7198
7199
7200
7201
7202
7203
7204
7205
7206
7207
7208
7209
7200
7201
7202
7203
7204
7205
7206
7207
7208
7209
7210
7211
7212
7213
7214
7215
7216
7217
7218
7219
7210
7211
7212
7213
7214
7215
7216
7217
7218
7219
7220
7221
7222
7223
7224
7225
7226
7227
7228
7229
7220
7221
7222
7223
7224
7225
7226
7227
7228
7229
7230
7231
7232
7233
7234
7235
7236
7237
7238
7239
7230
7231
7232
7233
7234
7235
7236
7237
7238
7239
7240
7241
7242
7243
7244
7245
7246
7247
7248
7249
7240
7241
7242
7243
7244
7245
7246
7247
7248
7249
7250
7251
7252
7253
7254
7255
7256
7257
7258
7259
7250
7251
7252
7253
7254
7255
7256
7257
7258
7259
7260
7261
7262
7263
7264
7265
7266
7267
7268
7269
7260
7261
7262
7263
7264
7265
7266
7267
7268
7269
7270
7271
7272
7273
7274
7275
7276
7277
7278
7279
7270
7271
7272
7273
7274
7275
7276
7277
7278
7279
7280
7281
7282
7283
7284
7285
7286
7287
7288
7289
7280
7281
7282
7283
7284
7285
7286
7287
7288
7289
7290
7291
7292
7293
7294
7295
7296
7297
7298
7299
7290
7291
7292
7293
7294
7295
7296
7297
7298
7299
7299
7300
7301
7302
7303
7304
7305
7306
7307
7308
7309
7300
7301
7302
7303
7304
7305
7306
7307
7308
7309
7310
7311
7312
7313
7314
7315
7316
7317
7318
7319
7310
7311
7312
7313
7314
7315
7316
7317
7318
7319
7320
7321
7322
7323
7324
7325
7326
7327
7328
7329
7320
7321
7322
7323
7324
7325
7326
7327
7328
7329
7330
7331
7332
7333
7334
7335
7336
7337
7338
7339
7330
7331
7332
7333
7334
7335
7336
7337
7338
7339
7340
7341
7342
7343
7344
7345
7346
7347
7348
7349
7340
7341
7342
7343
7344
7345
7346
7347
7348
7349
7350
7351
7352
7353
7354
7355
7356
7357
7358
7359
7350
7351
7352
7353
7354
7355
7356
7357
7358
7359
7360
7361
7362
7363
7364
7365
7366
7367
7368
7369
7360
7361
7362
7363
7364
7365
7366
7367
7368
7369
7370
7371
7372
7373
7374
7375
7376
7377
7378
7379
7370
7371
7372
7373
7374
7375
7376
7377
7378
7379
7380
7381
7382
7383
7384
7385
7386
7387
7388
7389
7380
7381
7382
7383
7384
7385
7386
7387
7388
7389
7390
7391
7392
7393
7394
7395
7396
7397
7398
7399
7390
7391
7392
7393
7394
7395
7396
7397
7398
7399
7399
7400
7401
7402
7403
7404
7405
7406
7407
7408
7409
7400
7401
7402
7403
7404
7405
7406
7407
7408
7409
7410
7411
7412
7413
7414
7415
7416
7417
7418
7419
7410
7411
7412
7413
7414
7415
7416
7417
7418
7419
7420
7421
7422
7423
7424
7425
7426
7427
7428
7429
7420
7421
7422
7423
7424
7425
7426
7427
7428
7429
7430
7431
7432
7433
7434
7435
7436
7437
7438
7439
7430
7431
7432
7433
7434
7435
7436
7437
7438
7439
7440
7441
7442
7443
7444
7445
7446
7447
7448
7449
7440
7441
7442
7443
7444
7445
7446
7447
7448
7449
7450
7451
7452
7453
7454
7455
7456
7457
7458
7459
7450
7451
7452
7453
7454
7455
7456
7457
7458
7459
7460
7461
7462
7463
7464
7465
7466
7467
7468
7469
7460
7461
7462
7463
7464
7465
7466
7467
7468
7469
7470
7471
7472
7473
7474
7475
7476
7477
7478
7479
7470
7471
7472
7473
7474
7475
7476
7477
7478
7479
7480
7481
7482
7483
7484
7485
7486
7487
7488
7489
7480
7481
7482
7483
7484
7485
7486
7487
7488
7489
7490
7491
7492
7493
7494
7495
7496
7497
7498
7499
7490
7491
7492
7493
7494
7495
7496
7497
7498
7499
7499
7500
7501
7502
7503
7504
7505
7506
7507
7508
7509
7500
7501
7502
7503
7504
7505
7506
7507
7508
7509
7510
7511
7512
7513
7514
7515
7516
7517
7518
7519
7510
7511
7512
7513
7514
7515
7516
7517
7518
7519
7520
7521
7522
7523
7524
7525
7526
7527
7528
7529
7520
7521
7522
7523
7524
7525
7526
7527
7528
7529
7530
7531
7532
7533
7534
7535
7536
7537
7538
7539
7530
7531
7532
7533
7534
7535
7536
7537
7538
7539
7539
7540
7541
7542
7543
7544
7545
7546
7547
7548
7549
7540
7541
7542
7543
7544
7545
7546
7547
7548
7549
7550
7551
7552
7553
7554
7555
7556
7557
7558
7559
7550
7551
7552
7553
7554
7555
7556
7557
7558
7559
7560
7561
7562
7563
7564
7565
7566
7567
7568
7569
7560
7561
7562
7563
7564
7565
7566
7567
7568
7569
7570
7571
7572
7573
7574
7575
7576
7577
7578
7579
7570
7571
7572
7573
7574
7575
7576
7577
7578
7579
7580
7581
7582
7583
7584
7585
7586
7587
7588
7589
7580
7581
7582
7583
7584
7585
7586
7587
7588
7589
7590
7591
7592
7593
7594
7595
7596
7597
7598
7599
7590
7591
7592
7593
7594
7595
7596
7597
7598
7599
7599
7600
7601
7602
7603
7604
7605
7606
7607
7608
7609
7600
7601
7602
7603
7604
7605
7606
7607
7608
7609
7610
7611
7612
7613
7614
7615
7616
7617
7618
7619
7610
7611
7612
7613
7614
7615
7616
7617
7618
7619
7620
7621
7622
7623
7624
7625
7626
7627
7628
7629
7620
7621
7622
7623
7624
7625
7626
7627
7628
7629
7630
7631
7632
7633
7634
7635
7636
7637
7638
7639
7630
7631
7632
7633
7634
7635
7636
7637
7638
7639
7639
7640
7641
7642
7643
7644
7645
7646
7647
7648<br

Figure 2



01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

Figure 2 (con't)

